CLAIMS

1. An intrusion detection system (6, 22) for detecting unauthorised use of a network (2, 20), comprising a sniffer (14) for capturing data being transmitted on said network and a pattern matching engine (16), receiving data captured by said sniffer (14) and comparing said data with attack signatures, for generating an event when a match between captured data and at least one attack signature is found, characterised in that said system further comprises a response analysis engine (18), triggered by said event, for comparing with response signatures the data being transmitted on said network as a response to said data matched with said attack signature, and for correlating the results of said comparisons with attack and response signatures for generating an alarm.

2. The system of claim 1, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by said sniffer (14) by performing an analysis of source IP address in data packets transmitted on said network.

3. The system of claim 1, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by said sniffer (14) by performing an analysis of both source and destination IP addresses in data packets transmitted on said network.

4. The system of claim 1, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by said sniffer (14) by analysing transport level information in data packets transmitted on said network.

5. The system of claim 1, wherein said response analysis engine (18) generates an alarm when said data being transmitted on said network as a response to said data matched with said attack signature indicates that a new network connection has been established.

6. The system of claim 1, wherein said response signatures are arranged in two categories, type A response signatures identifying an illicit traffic, and type B response signatures identifying legitimate traffic.

7. The system of claim 6, wherein said response analysis engine (18) generates an alarm when a match between captured data and a response signature identifying illicit traffic (type A) is found.

8. The system of claim 6, wherein said response analysis engine (18) comprises a counter (num_pos_match) which is incremented when a match between captured data and a response signature identifying legitimate traffic (type B) is found.

9. The system of claim 8, wherein, when said counter (num_pos_match) reaches a predetermined value (req(signatures)), said response analysis engine (18) terminates without generating any alarm (62).

10. The system of claim 1, wherein said response analysis engine (18) comprises a time-out system (64), triggered by said event, for starting a probing task (52).

11. The system of claim 10, wherein said probing task (52) verifies if any data has been detected on said network as a response to said data matched with said attack signature, and, if such condition is verified:

- generates an alarm in case only response signatures indicating legitimate traffic (type B) have been used by said response analysis engine (18); or
- ends the probing task (82) in case only response signatures indicating illicit traffic (type A) or both response signatures indicating legitimate traffic (type B) and illicit traffic (type A) have been used by said response analysis engine (18).

12. The system of claim 11, wherein, if such condition is not verified, said probing task (52) attempts to perform a connection (76) to a suspected attacked computer, for generating an alarm (80) if such attempt is successful, or for ending the probing task (82) if such attempt is unsuccessful.

13. A method for detecting unauthorised use of a network, comprising the steps:
- capturing data being transmitted on said network;
- comparing said data with attack signatures, for generating an event when a match between captured data and at least one attack signature is found;
characterised in that it comprises, triggered by said event, the steps of:
- comparing with response signatures the data being transmitted on said network as a response to said data matched with said attack signature;
- correlating the results of said comparisons with attack and response signatures for generating an alarm.

14. The method of claim 13, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by performing an analysis of source IP address in data packets transmitted on said network.

15. The method of claim 13, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by performing an analysis of both source and destination IP addresses in data packets transmitted on said network.

16. The method of claim 13, wherein said data being transmitted on said network as a response to said data matched with said attack signature is captured by analysing transport level information in data packets transmitted on said network.

17. The method of claim 13, comprising the step of generating an alarm when said data being transmitted on said network as a response to said data matched with said attack signature indicates that a new network connection has been established.

18. The method of claim 13, wherein said response signatures are arranged in two categories, type A response signatures identifying an illicit traffic, and type B response signatures identifying legitimate traffic.

19. The method of claim 18, comprising the step of generating an alarm when a match between captured data and a response signature identifying illicit traffic (type A) is found.

20. The method of claim 18, comprising the step of incrementing a counter (num_pos_match) when a match between captured data and a response signature identifying legitimate traffic (type B) is found.

21. The method of claim 20, wherein said step of comparing data with response signatures is terminated when said counter (num_pos_match) reaches a predetermined value (req(signatures)).

22. The method of claim 13, comprising the step of providing a time-out system (64), triggered by said event, for starting a probing task (52).

23. The method of claim 22, comprising the step of verifying if any data has been detected on said network as a response to said data matched with said attack signature, and, if such condition is verified:

- generating an alarm in case only response signatures indicating legitimate traffic (type B) have been used; or
- ending said probing task (82) in case only response signatures indicating illicit traffic (type A) or both response signatures indicating legitimate traffic (type B) and illicit traffic (type A) have been used.

24. The method of claim 23, wherein, if such condition is not verified, said probing task (52) attempts to perform a connection (76) to a suspected attacked computer, for generating an alarm (80) if such attempt is successful, or for ending the probing task (82) if such attempt is unsuccessful.

25. A computer program product loadable in the memory of at least one computer and including software code portions for performing the method of any of claims 13 to 24 when the product is run on a computer.